Privacy Policy

Last updated: **01/07/2026**

Tutto Media, LLC (dba ISO Connections) ("**Company**", "**we**", "**our**", or "**us**") respect your privacy and are committed to protecting it through our compliance with this policy. This policy describes how we collect, process, retain, and disclose personal data about you when providing services to you through our websites, and services that link to this policy (our "**Services**") and our practices for using, maintaining, protecting, and disclosing that information.

This policy applies only to information we collect:

- Through the Services.
- In communications, including email, text, chat, and other electronic messages, between you and the Services.
- When you interact with our advertising and applications (including mobile apps) on third-party websites and services, if those applications or advertising include links to this policy.

It does not apply to information collected by:

- Us offline or through any other means, including on any other website operated by Company or any third party (including our affiliates and subsidiaries) that does not link to this policy; or
- Any third party (including our affiliates and subsidiaries), including through any application or content (including advertising) that may link to or be accessible from or through the Services.

We may provide additional or different privacy policies that are specific to certain features, services, or activities.

Please read this policy carefully to understand our policies and practices regarding your information and how we treat it. By interacting with our Services or providing us with your information, you agree to the collection, use, and sharing of your information as described in this privacy policy. This policy may change from time to time (see "How We Retain Your Personal Data"). Your continued use of the Services after we make changes as described here is deemed to be acceptance of those changes, so please check the policy periodically for updates.

Children's and Minors' Data

Our Services are not intended for, and we do not knowingly collect any personal data from, children under the age of 18. If we learn we have collected or received personal data from a child under 18 years old without verification of parental consent, we will delete that information.

The Personal Data That We Collect or Process

"**Personal data**" is information that identifies, relates to, or describes, directly or indirectly, you as an individual, such as your name, email address, telephone number, or home

address (for example, account information such as name, postal address, and email address, or social security number or any other identifier we may use to contact you online or offline).

The types and categories of personal data we may collect or process include:

- Account and contact information, including name, address (such as home address, work address, or other address), email address, phone number, username, and other contact information you provide us.
- Account history, including information about your account, and transactions.
- Demographic information, including your age, gender, income level, education, or family or marital status, if you have consented to such information collection.
- Location information, including general geographic location such as country, state or province, or city and precise geolocation, if you have enabled and consented to location information collection.
- Content and information you elect to provide as part of your profile or in any reviews you make through the Services or emails, chats, or other communications sent to us.
- Images, voice recordings, and videos collected or stored in connection with the Services, if you have consented to such information collection.

Some of the information identified above may be considered sensitive data under certain laws. If required under applicable law, we will collect and process sensitive personal data only with your consent. If you choose not to provide or allow us to collect some information, we may not be able to provide you with requested features, services, or information.

We also collect:

- **Statistics or aggregated information.** Statistical or aggregated data does not directly identify a specific person, but we may derive non-personal statistical or aggregated data from personal data. For example, we may aggregate personal data to calculate the percentage of users accessing a specific Services feature.

If we combine or connect non-personal statistical with personal data so that it directly or indirectly identifies an individual, we treat the combined information as personal information.

How We Collect Your Personal and Other Data

You Provide Information to Us

We collect information about you when you interact with our Services, such as when you create or update an account, make a request, participate in surveys, sweepstakes, contests, or promotions, or create, upload, or post content to the Services, including reviews, media such as photos, videos, or audio recordings.

Automatically Through Our Services

As you navigate through and interact with our Services, we may use automatic data collection technologies to collect information that may include personal data. Information

collected automatically may include usage details, IP addresses, operating system, and browser type, and information collected through cookies, web beacons, and other tracking technologies including details of your interactions with our Services, such as traffic data, location data, logs, and other communication data, and which resources and Services features that you access and use.

We may use these automatic collection technologies to collect information about your online activities over time and across third-party sites or other online services (behavioral tracking).

Using automatic collection technologies helps us to improve our Services and to deliver a better and more personalized experience.

The technologies we use for this automatic data collection may include:

- **Cookies.** A cookie is a small file placed on your device when you interact with the Services. You may refuse to accept or disable cookies by activating the appropriate setting on your browser or device. However, if you select this setting, you may be unable to access certain features of the Services.
- **Web Beacons.** Some parts of the Services and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those parts or opened an email and for other related statistics (for example, recording the popularity of certain content and verifying system and server integrity).

To the extent any of these automated technologies are considered a personal data sale, targeted advertising, or profiling, under applicable laws, depending on where you live, you may opt out from use of these automated technologies for such uses. Please note that some Services features may be unavailable as a result.

When you interact with the Services, there are third parties that may use automatic collection technologies to collect information about your or your device. These third parties may include:

- Advertisers, ad networks, and ad servers.
- Analytics companies.
- Your device manufacturer.
- Your internet or mobile service provider.

These third parties may use tracking technologies to collect information about you when you use the Services. The information they collect may be associated with your personal data or they may collect information, including personal data, about your online activities over time and across different websites, apps, platforms, and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content.

We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

From Business Partners and Service Providers

We may receive personal data about you from other sources and combine that with information we collect directly from you. For example, we may obtain information about you from service providers that we engage to perform services on our behalf, such as email platform providers, content delivery services, payment processors, promotions services, gift card program providers, analytics, security and anti-fraud services, and data brokers. We also may receive personal data from business partners that we engage to share consumer information with us, including your personal preferences and demographic information such as age, gender, and income level so that we can better provide you with a personalized experience, including personalized content, offers and services.

How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal data, to:

- Provide you with the Services and any contents, features, information, products, or services that we make available through the Services, including not by limitation sharing your personal information with third parties as a lead service provider.
- Fulfill any other purpose for which you provide it.
- Provide you with notices about your account, including expiration and renewal notices.
- Improve our Services, including by analyzing your information and creating aggregated data derived from your information) to develop, maintain, analyze, improve, optimize, measure, and report on our Services and their features and how users interact with them. Our analysis may include the use of technology like machine learning and large language models, which may include training these models or sharing with third parties for model training.
- Promote our Services, business, and offerings by publishing advertising on our own Services and by placing ads on third parties' services. We may use your information to model, segment, target, offer, market, and advertise our Services.
- Carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- Notify you when Services updates are available and about changes to any products or services we offer or provide though them.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

The usage information we collect, whether connected to your personal data or not, helps us improve our Services and deliver a better and more personalized experience by enabling us to:

- Estimate our audience sizes and usage patterns.

- Store information about your preferences, allowing us to customize the Services according to your individual needs and interests.
- Speed up your searches.
- Recognize you when you return to our Services.

We may also use your information to contact you about goods and services that may be of interest to you. If you do not want us to use your information in this way, please check the relevant box located on the form on which we collect your data (the registration form) For more information, see Your Rights and Choices About Your Information.

Who We Disclose Your Information To

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may also disclose personal data that we collect or you provide as described in this privacy policy:

- To third-party contractors so they can contact you.
- To our subsidiaries and affiliates.
- To contractors, service providers, and other third parties we use to support our organization.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Tutto Media, LLC (dba ISO Connections)'s assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by Tutto Media, LLC (dba ISO Connections) is among the assets transferred.
- To third parties to market their products or services to you if you have consented to these disclosures. For more information, see Your Rights and Choices About Your Information.
- To fulfill the purpose for which you provide it. For example, if you give us an email address to use the "email a friend" feature of our Services, we will transmit the contents of that email and your email address to the recipients.
- For any other purpose disclosed by us when you provide the information.
- With your consent.

We may also disclose your personal data:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request.
- To enforce or apply our agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or

safety of our organization, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

Your Rights and Choices About Your Information

This section describes mechanisms you can use to control certain uses and disclosures of your information and rights you may have under state law, depending on where you live.

Advertising, marketing, cookies, and other tracking technologies choices:

- **Cookies and Other Tracking Technologies.** You can set your browser to refuse all or some browser cookies or other tracking technology files, or to alert you when these files are being sent. You can choose whether or not to allow the Services to collect information through other tracking technologies. If you disable or refuse cookies or similar tracking files, some Services features may be inaccessible or not function properly. Some browsers include a "Do Not Track" (DNT) setting that can send a signal to the online services you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our Services may not respond to all browser DNT signals. Instead, you can use the range of other tools to control data collection and use, including the cookie controls and advertising controls described in this policy.
- **Promotions by the Company.** If you do not wish us to use your information to promote our own or third parties' products or services, you can opt out by sending us an email stating your request to *www.isoconnection.net/contact*.
- **Targeted Advertising by the Company.** If you do not want us to use information that we collect or that you provide to us to deliver advertisements according to our advertisers' target audience preferences, you can opt out by sending us an email stating your request to *www.isoconnection.net/contact*. For this opt out to function, you must have your browser set to accept all browser cookies.
- **Disclosure of Your Information for Third-Party Advertising.** If you do not want us to share your personal data with unaffiliated or non-agent third parties for advertising and marketing purposes, you can opt out by sending us an email stating your request to *www.isoconnection.net/contact*. We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. To learn more about opting out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**"), including how to add the NAI Global Privacy Control (GPC) extension to your Chrome web browser, see NAI: How to Opt Out.

Location data choices:

- **Location Data.** You can choose whether or not to allow the Services to collect and use

real-time information about your device's location through the device's privacy settings or sending us an email stating your request to *www.isoconnection.net/contact*. If you block the use of location information, some Services features may become inaccessible or not function properly.

Your State Privacy Rights

Depending on your state of residency, you may have certain rights related to your personal data, including:

- **Access and Data Portability.** You may confirm whether we process your personal data and access a copy of the personal data we process. To the extent feasible, data will be provided in a portable format. Depending on your state, you may have the right to receive additional information and it will be included in the response to your access request.
- **Correction.** You may request that we correct inaccuracies in your personal data that we maintain, taking into account the information's nature and processing purpose.
- **Deletion.** You may request that we delete personal data about you that we maintain, subject to certain exception under applicable law.
- **Opt Out of Using Personal Data for Targeted Advertising, Profiling, and Sales.** You may request that we do not use your personal data for these purposes.

Important: The exact scope of these rights vary by state. There are also several exceptions where we may not have an obligation to fulfill your request.

To exercise any of these rights, please send us an email stating your request to *www.isoconnection.net/contact*.

Some browsers and browser extensions support the Global Privacy Control ("**GPC**") that can send a signal to process your request to opt out from certain types of data processing, including data "sales" as defined under certain laws. When we detect such a signal, we will make reasonable efforts to respect your choices indicated by a GPC setting as required by applicable law.

How We Protect Your Personal Data

We use commercially reasonable administrative, physical, and technical measures designed to protect your personal data from accidental loss or destruction and from unauthorized access, use, alteration, and disclosure. However, no website, mobile application, system, electronic storage, or online service is completely secure, and we cannot guarantee the security of your personal data transmitted to, through, using, or in connection with the Services. In particular, email, texts, and chats sent to or from the Services may not be secure, and you should carefully decide what information you send to us via such communications channels. Any transmission of personal data is at your own risk.

The safety and security of your information also depends on you. You are responsible for taking steps to protect your personal data against unauthorized use, disclosure, and access.

How We Retain Your Personal Data

We keep the categories of personal data described in this policy for as long as reasonably necessary to fulfill the purposes described or for as otherwise legally permitted or required, such as maintaining the Services, operating our organization, complying with our legal obligations, resolving disputes, and for safety, security, and fraud prevention. This means that we consider our legal and business obligations, potential risks of harm, and nature of the information when deciding how long to retain personal data. At the end of the retention period, personal data will be deleted, destroyed, or deidentified.

Changes to Our Privacy Policy

We may update this policy from time to time, and we will provide notice of any such changes to the policy as required by law. The date the privacy policy was last updated is identified at the top of the page. We will notify you of changes to this policy by updating the "last updated" date and posting the updated policy on the Services. We may email or otherwise communicate reminders about this policy, but you should check our Services periodically to see the current policy and any changes we have made to it.

Contact Information

To exercise your rights or ask questions or comment about this Privacy Policy or our privacy practices, contact us at: *www.isoconnection.net/contact*.

To register a complaint or concern, please send us an email stating your request to *www.isoconnection.net/contact*.

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

The objectives of this comprehensive written information security program ("**WISP**") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards TUTTO MEDIA, LLC ("**Company**") has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of N.Y. Gen. Bus. Law 899-aa & 899-bb, and other similar US and state laws, as applicable.

If this WISP conflicts with any legal obligation or other Company policy or procedure, the provisions of this WISP shall govern, unless the Information Security Coordinator specifically reviews, approves, and documents an exception (see Section 3).

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity, and availability of personal and other Sensitive Information Company collects, creates, uses, and maintains.

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

(c) Protect against unauthorized access to or use of Company-maintained personal and other Sensitive Information that could result in substantial harm or inconvenience to any customer or employee.

(d) Define an information security program that is appropriate to Company's size, scope, and business, its available resources, and the amount of personal and other Sensitive Information that Company owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

2. Scope. This WISP applies to all members, employees, and contractors of Company. It applies to any records that contain personal or other Sensitive Information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "**personal information**" means either a US resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account.

(iv) Health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by Company;

(v) Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;

(vi) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or

(vii) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records.

(c) For purposes of this WISP, "**sensitive information**" means data that:

(i) Company considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to Company, its customers, or its business partners.

(iii) Sensitive information includes, but is not limited to, personal information.

3. Information Security Coordinator. Company has designated ANDREW VALITUTTO, Member of Company, to implement, coordinate, and maintain this WISP (the "**Information Security Coordinator**"). The Information Security Coordinator shall be responsible for:

(a) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to personal and other sensitive information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);

(ii) Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);

(iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal and other sensitive information (see Section 6);

(iv) Ensuring that the safeguards are implemented and maintained to protect personal and other sensitive information throughout Company, where applicable (see Section 6);

(v) Overseeing service providers that access or maintain personal and other sensitive information on behalf of Company (see Section 7);

(vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);

(vii) Defining and managing incident response procedures (see Section 9); and

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with Company human resources and management (see Section 10).

(b) Engaging qualified information security personnel, including:

(i) Providing them with security updates and training sufficient to address relevant risks; and

(ii) Verifying that they take steps to maintain current information security knowledge.

(c) Employee, contractor, and (as applicable) stakeholder training, including:

(i) Providing periodic training regarding this WISP, Company's safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal or other sensitive information, updated as necessary or indicated by Company's risk assessment activities (see Section 4);

(ii) Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation; and

(iii) Retaining training and acknowledgment records.

(d) Reviewing this WISP and the security measures defined here at least annually, when indicated by Company's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), or whenever there is a material change in Company's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information (see Section 11).

(e) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or Company's information security policies and procedures.

(f) Periodically, but at least annually, reporting to Company's management regarding the status of the information security program and Company's safeguards to protect personal and other sensitive information, including the program's overall status, compliance with applicable laws and regulations, material matters related to the program, such as risk assessment, risk management and control decisions, service provider arrangements, testing results, cyber incidents or policy violations and management's responses, and recommendations for program changes.

4. Risk Assessment. As a part of developing and implementing this WISP, Company will conduct and base its information security program on a periodic, documented risk assessment, at least annually, or whenever there is a material change in Company's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal or other sensitive information and include criteria for evaluating and categorizing those identified risks;

(ii) Define assessment criteria and assess the likelihood and potential damage that could result from such risks, including the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the personal or other sensitive information, taking into consideration the sensitivity of the personal and other sensitive information; and

(iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Employee, contractor, and (as applicable) stakeholder training and management;

(B) Employee, contractor, and (as applicable) stakeholder compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

(D) Company's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, Company will:

(i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

(ii) Reasonably and appropriately address any identified gaps, including documenting Company's plan to remediate, mitigate, accept, or transfer identified risks, as appropriate; and

(iii) Regularly monitor the effectiveness of Company's safeguards, as specified in this WISP (see Section 8).

5. Information Security Policies and Procedures. As part of this WISP, Company will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for personal and other sensitive information, including the storage, access, disposal, and external transfer or transportation of personal and other sensitive information;

(iii) User access management, including identification and authentication (using passwords or other appropriate means);

(iv) Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD); and

(ix) Information systems acquisition, development, operations, and maintenance.

(b) Detail the implementation and maintenance of Company's administrative, technical, and physical safeguards (see Section 6).

6. Safeguards. Company will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal or other sensitive information that Company owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to Company's size, scope, and business, its available resources, and the amount of personal and other sensitive information that Company owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

(b) Company shall document its administrative, technical, and physical safeguards in Company's information security policies and procedures (see Section 5).

7. Service Provider Oversight. Company will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal or other sensitive information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and Company's obligations.

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and Company's obligations.

(c) Monitoring and periodically auditing the service provider's performance to verify compliance with this WISP and all applicable laws and Company's obligations.

8. Monitoring. Company will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal or other sensitive information. Company shall reasonably and appropriately address any identified gaps.

9. Incident Response. Company will establish and maintain written policies and procedures regarding information security incident response (see Section 5). Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security.

(b) Performing a post-incident review of events and actions taken.

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP will result in disciplinary action, in accordance with Company's information security policies and procedures and human resources policies. Please see Company's Employee Handbook for details regarding Company's disciplinary process.

11. Program Review. Company will review this WISP and the security measures defined herein at least annually, when indicated by Company's risk assessment (see Section 4) or program monitoring and testing activities (see Section 8), or whenever there is a material change in Company's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

(a) Company shall retain documentation regarding any such program review, including any identified gaps and action plans.

12. Effective Date. This WISP is effective as of **01/07/2026**

(a) Revision History:

(i) Original publication: **01/07/2026**

CYBER INCIDENT RESPONSE PLAN (IRP)

1. Purpose and Goals. The purpose of this cyber incident response plan ("**IRP**") is to provide a structured and systematic incident response process for all information security incidents (as defined in Section 4, Definitions) that affect any TUTTO MEDIA, LLC ("**Company**") information technology ("**IT**") systems or operational technology ("**OT**") systems, network, or data, including Company's data held or IT or OT services provided by third-party vendors or other service providers.

1.1 Specifically, Company's goals for this IRP include to:

(a) Define Company's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist Company and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.

(c) Mitigate or minimize the effects of any information security incident on Company, its clients, employees, or others.

(d) Help Company consistently document the actions it takes in response to information security incidents.

(e) Reduce overall risk exposure for Company.

(f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in Company's information security program and incident response process.

1.2 Company developed and maintains this IRP as may be required by applicable laws and regulations.

2. Scope. This IRP applies to all Company members, employees, and contractors; and Company's IT and OT systems, network, data, and any computer systems or networks connected to Company's network.

2.1 Other Plans and Policies. Company may, from time to time, approve and make available more detailed or location or work group-specific plans, policies, procedures, standards, or processes to address specific information security issues or incident response procedures. Those additional plans, policies, procedures, standards, and processes are extensions to this IRP. You may find and obtain approved information security policies, including Company's Written Information Security Program ("**WISP**"), and other resources from Company's Business Manager.

3. Accountability. Company has designated ANDREW VALITUTTO, Member of Company, to implement and maintain this IRP (the "**Information Security Coordinator**").

3.1 Information Security Coordinator Duties. Among other information security duties, as defined in Company's WISP, the Information Security Coordinator shall be responsible for:

(a) Implementing this IRP.

(b) Identifying the incident response team ("**IRT**") and any appropriate sub-teams to address specific information security incidents, or categories of information security incidents (see Section 5, Incident Response Team).

(c) Coordinating IRT activities, including developing, maintaining, and following appropriate procedures to respond to, appropriately escalate, make decisions regarding, and document identified information security incidents (see Section 6, Incident Response Procedures).

(d) Conducting post-incident reviews to gather feedback on information security incident response procedures and address any identified gaps in security measures (see Section 6.7, Post-Incident Review).

(e) Providing training and conducting periodic exercises to promote employee and stakeholder preparedness and awareness of this IRP (see Section 7, Plan Training and Testing).

(f) Reviewing this IRP at least annually, or whenever there is a material change in Company's business practices that may reasonably affect its cyber incident response procedures (see Section 8, Plan Review).

3.2 Enforcement. Violations of or actions contrary to this IRP may result in disciplinary action, in accordance with Company's information security policies and procedures and human resources policies. Please see Company's Employee Handbook for details regarding Company's disciplinary process.

4. Definitions. The terms defined below apply throughout this IRP:

4.1 "**Confidential Information**." Confidential information means information as defined in Company's WISP that may cause harm to Company or its clients, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available.

4.2 "**Personal Information**." Personal information means individually identifiable information as defined in Company's WISP that Company owns, licenses, or maintains and that is from or about an individual including, but not limited to (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online information, such as a user name and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card

account number; (g) date of birth; (h) health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by Company; and (i) any information that is combined with any of (a) through (h) above.

4.3 "**Information Security Incident**." Information security incident means an actual or reasonably suspected (a) loss or theft of confidential or personal information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of confidential or personal information that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of Company's IT or OT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information or Company's operating environment or services.

5. Incident Response Team. The incident response team is a predetermined group of Company employees and resources responsible for responding to information security incidents.

5.1 Role. The IRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to Company's IT systems, network, and data; (b) minimize economic, reputational, or other harms to Company and its clients, employees, and partners; and (c) manage litigation, enforcement, and other risks.

5.2 Authority. Through this IRP, Company authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this IRP.

5.3 Responsibilities. The IRT is responsible for:

(a) Addressing information security incidents in a timely manner, according to this IRP.

(b) Managing internal and external communications regarding information security incidents.

(c) Reporting its findings to management and to applicable authorities, as appropriate.

(d) Reprioritizing other work responsibilities to permit a timely response to information security incidents on notification.

5.4 IRT Roster. The IRT consists of a core team, led by the Information Security Coordinator. The current IRT roster includes the following individuals:

ANDREW VALITUTTO, Member of Company and Information Security Coordinator, (845) 293-3090.

(a) Sub-Teams and Additional Resources. The Information Security Coordinator assigns and coordinates the IRT for any specific information security incident according to incident characteristics and Company needs. The Information Security Coordinator may:

(i) Identify and maintain IRT sub-teams to address specific information security incidents, or categories of information security incidents.

(ii) Call on external individuals, including vendor, service provider, or other resources, to participate in specific-event IRTs, as necessary.

6. Incident Response Procedures. Company shall develop, maintain, and follow incident response procedures as defined in this Section 6 to respond to and document identified information security incidents.

Company recognizes that following initial escalation, the information security incident response process is often iterative, and the steps defined in Sections 6.3, Investigation and Analysis; 6.4, Containment, Remediation, and Recovery; 6.5, Evidence Preservation; and 6.6, Communications and Notification may overlap or the IRT may revisit prior steps to respond appropriately to a specific information security incident.

Company may, from time to time, approve and make available more specific procedures for certain types of information security incidents. Those additional procedures and checklists are extensions to this IRP. You may find and obtain approved information security policies and other resources from Company's Business Manager.

6.1 Detection and Discovery. Company shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.

(a) Automated Detection. Company shall develop, implement, and maintain automated detection means and other technical safeguards as described in Company's WISP.

(b) Reports from Employees or Other Internal Sources. Employees, or others authorized to access Company's IT or OT systems, network, or data, shall immediately report any actual or suspected information security incident to any member of the IRT. Individuals should report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to any member of the IRT. Employees who receive emails or other communications from external sources regarding information security incidents that may affect Company or others, security vulnerabilities, or related issues shall immediately report those communications to any member of the IRT and shall not interact with the source unless authorized.

(d) Assessing Potential Incidents. Company shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. Company shall document each identified information security incident, with initial details, as determined by the IRT.

6.2 Escalation. Following identification of an information security incident, the Information Security Coordinator, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to Company and its clients, employees, or others.

Based on the initial assessment, the Information Security Coordinator, or a designate, shall:

(a) IRT Activation. Notify and activate the IRT, or a sub-team, including any necessary external resources (see Section 5.4, IRT Roster).

As determined by the Information Security Coordinator.

(b) IRT Expectations. Set expectations for IRT member reply and engagement.

As determined by the Information Security Coordinator.

(c) Initial Notifications. Notify (if necessary) organizational leadership and any applicable business partners or service providers, Company's cyber insurance carrier, and law enforcement or other authorities (see Section 6.6, Communications and Notifications).

(d) Determine Decision-Making Authority. Following initial notifications, work with organizational leadership (if necessary) to establish any decision-making authority levels according to the information security incident's specific facts and circumstances. The Information Security Coordinator shall have decision-making authority regarding information security incidents.

6.3 Investigation and Analysis. On activation, the IRT shall collaborate to investigate each identified information security incident, analyze its effects, and formulate an appropriate response plan to contain, remediate, and recover from the incident.

The IRT shall document its investigation and analysis for each identified information security incident.

As determined by the Information Security Coordinator.

6.4 Containment, Remediation, and Recovery. Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to

contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources (see Section 6.3, Investigation and Analysis).

The IRT shall document its response plans and the activities completed for each identified information security incident.

As determined by the Information Security Coordinator.

6.5 Evidence Preservation. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities (see Sections 6.3, Investigation and Analysis and 6.4, Containment, Remediation, and Recovery). The IRT shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

As determined by the Information Security Coordinator.

6.6 Communications and Notifications. For each identified information security incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the IRT may authorize information security incident-related communications or notifications. The IRT shall seek counsel's advice, as needed, to review communications and notifications targets, content, and protocols.

(a) Internal Communications. The IRT shall prepare and distribute any internal communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Organizational Leadership. The IRT shall alert organizational leadership to the incident and explain its potential impact on Company, its clients, employees, and others as details become available.

(ii) General Awareness and Resources. As appropriate, the IRT shall explain the incident to Company's employees and other stakeholders and provide them with resources to appropriately direct questions from clients, media, or others.

(b) External Communications. The IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Public Statements. If Company determines that external statements are necessary, the IRT shall provide consistent, reliable information to the media and public regarding the incident using Company's website, press releases, or other means.

(ii) Law Enforcement. The IRT shall report criminal activity or threats to applicable authorities, as Company deems appropriate.

(c) Notifications. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require Company to notify various parties of some information security incidents. If applicable to a specific information security incident, as required, the IRT shall:

(i) Authorities. Notify applicable regulators, law enforcement, or other authorities.

(ii) Affected Individuals. If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

(iii) Cyber Insurance Carrier. Notify Company's cyber insurance carrier according to the terms and conditions of its current policy, including filing a claim, if appropriate.

(iv) Others. If applicable, notify clients or business partners according to current agreements.

6.7 Post-Incident Review. At a time reasonably following each identified information security incident, the Information Security Coordinator, or a designate, shall reconvene the IRT, others who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and Company's response.

(a) Review Considerations. The post-incident review team shall consider Company's effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

(b) Report. The post-incident review team shall document its findings.

(c) Follow-Up Actions. The Information Security Coordinator shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from Company leadership.

7. Plan Training and Testing.

7.1 Training. The Information Security Coordinator shall develop, maintain, and deliver training regarding this IRP that periodically, but at least annually:

(a) Informs all employees, and others who have access to Company's IT or OT systems, network, or data, about the IRP and how to recognize and report potential information security incidents.

(b) Educates IRT members on their duties and expectations for responding to information security incidents.

The Information Security Coordinator may choose to include training on this IRP in other information security training activities as defined in Company's WISP.

7.2 Testing. The Information Security Coordinator shall coordinate exercises to test this IRP periodically, but at least annually. The Information Security Coordinator shall document test results, lessons learned, and feedback and address them in plan reviews (see Section 8, Plan Review).

8. Plan Review. Company will review this IRP at least annually, or whenever there is a material change in Company's business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The Information Security Coordinator must approve any changes to this IRP and is responsible for communicating changes to affected parties.

Send any suggested changes or other feedback on this IRP to the Information Security Coordinator.

9. Effective Date. This IRP is effective as of 01/07/2026

9.1 Revision History.

(a) Original publication: 01/07/2026